WHAT IS CLAIMED IS:

1. A network intrusion detection system, comprising:

a processor;

a memory accessible by the processor;

a monitor application stored in the memory and executable by the processor, the monitor application adapted to monitor network activity associated with a network node;

a profile application stored in the memory and executable by the processor, the profile application adapted to automatically generate an activity profile associated with the network node using the monitored network activity; and

a recognition engine stored in the memory and executable by the processor, the recognition engine adapted to compare a network event to the activity profile to determine whether the network event is authorized for the network node.

2. The system of Claim 1, wherein the network activity comprises inbound data communications and outbound data communications.

3. The system of Claim 2, wherein the inbound and outbound data communications comprise electronic mail communications.

4. The system of Claim 2, wherein the inbound and outbound data communications comprise Internet communications.

5. The system of Claim 1, wherein the profile application generates the activity profile corresponding to network activity occurring over a predetermined time period.

6. The system of Claim 1, wherein the profile application is further adapted to automatically update the activity profile in response to a predetermined event.

7. The system of Claim 1, wherein the profile application is further adapted to automatically update the activity profile corresponding to a predetermined time period.

8. The system of Claim 1, wherein the recognition engine is further adapted to block the network event if the network event exceeds the activity profile.

9. The system of Claim 1, wherein the profile application is further adapted to automatically update the activity profile if the network event is authorized.

10. The system of Claim 1, further comprising an event library accessible by the recognition engine to determine whether the network event is authorized, the event library comprising information associated with authorized network activities not reflected in the activity profile.

11. A method for network intrusion detection, comprising:

monitoring network activity associated with a network node for a predetermined time period;

automatically generating an activity profile corresponding to the network node using the monitored network activity;

identifying a network event associated with the network node; and

automatically determining whether the network event is authorized for the network node using the activity profile.

12. The method of Claim 11, wherein monitoring the network activity comprises monitoring inbound data communications and outbound data communications associated with the network node.

13. The method of Claim 11, wherein monitoring the network activity comprises monitoring network application usage corresponding to the network node.

14. The method of Claim 11, further comprising accessing an event library to determine whether the network event is authorized, the event library comprising information associated with authorized network activities not reflected in the activity profile.

15. The method of Claim 11, further comprising automatically updating the activity profile if the network event is authorized.

16. The method of Claim 11, further comprising automatically blocking the network event if the network event is not authorized.

17. The method of Claim 11, further comprising automatically updating the activity profile in response to a predetermined network event.

18. The method of Claim 11, further comprising automatically updating the activity profile corresponding to a predetermined time period.

19 A network detection intrusion system, comprising:

a plurality of nodes coupled to a server via a network;

a monitoring application accessibly by the server and adapted to monitor network activity between the plurality of nodes;

a profile application accessible by the server and adapted to generate an activity profile for each of the plurality of nodes; and

a recognition engine accessible by the server and adapted to compare a network event corresponding to one of the plurality of nodes to the activity profile corresponding to the one node to determine whether the network event is authorized for the one node.

20. The system of Claim 19 wherein the profile application is further adapted to automatically update the activity profile corresponding to the one node if the network event is authorized.

21. The system of Claim 19 wherein the monitoring application is adapted to monitor inbound data communications and outbound data communications associated with each of the nodes.

22. The system of Claim 19 further comprising an event library accessible by the server to determine whether the network event is authorized, the event library comprising information associated with authorized network activities not reflected in the activity profile for the one node.

23. The system of Claim 19 wherein the monitoring application is adapted to monitor network application usage for each of the nodes.

24. The system of Claim 19 wherein the recognition engine is further adapted to generate an event alarm log for the network event if the network event is not authorized.

25. The system of Claim 19, wherein the profile application is further adapted to automatically update the activity profile for each of the nodes corresponding to a predetermined time period.

26. The system of Claim 19, wherein the profile application is further adapted to automatically update an activity profile corresponding to a node in response to a predetermined network event corresponding to the node.

27. A computer program for assisting in network intrusion detection, comprising:

a computer-readable medium; and

a profile application stored on the computer-readable medium, the profile application adapted to monitor network activity and generate an activity profile using the monitored network activity, the activity profile used to determine whether a network event is authorized.

28. The computer program of Claim 27, wherein the profile application is configured to automatically update the activity profile in response to a predetermined network event.

29. The computer program of Claim 27, wherein the profile application is further configured to automatically update the activity profile corresponding to a predetermined time interval.

30. The computer program of Claim 27, further comprising a recognition engine stored on the computer-readable medium and adapted to compare the network event to the activity profile.

31. The computer program of Claim 27, wherein the profile application is adapted to monitor inbound data communications and outbound data communications corresponding to the network.

32. The computer program of Claim 27, further comprising a recognition engine adapted to compare the network event to the activity profile and block the network event if the network event exceeds the activity profile.

33. The computer program of Claim 27, wherein the profile application generates the activity profile corresponding to network activity occurring over a predetermined time period.